REMARKS

The enclosed is responsive to Examiner's Final Office Action mailed on February 1, 2008. At the time Examiner mailed the Final Office Action claims 29-36 and 67-82 were pending. By way of the present response Applicant has amended no claims; cancelled no claims; and added no new claims. As such, claims 29-36 and 67-82 are now pending. Applicants respectfully request reconsideration of the present application and the allowance of all claims now presented.

Claim Rejections – 35 USC §103

Claims 29-36 and 67-82 are rejected under 35 U.S.C. 103(a) as being unpatentable over Morkel, U.S. Patent No. 7,007,068 B2 (hereinafter "Morkel") in view of Ben Livingston , possible modifications to Washington, anti-spam law, Internet Newsgroup, January 31, 2002, (hereinafter "Livingston") further in view of Russell, U.S. Patent No. 7,099,444 B1 (hereinafter "Russell").

Claims 80-82 are rejected under 35 U.S.C. 103(a) as being unpatentable over Morkel in view of Livingston further in view of Russell further in view of U.S. Patent No. 7,174,453 (hereinafter "Lu").

Applicant does not admit Russell is prior art

Applicant does not admit that Russell is prior art and reserves the right of argument in a future response (e.g., an appeal). Russell, filed April 15, 2004, claims priority to provisional application no. 60/463,706, filed on April 16, 2003. Thus, Applicant's filing date (September 24, 2003) is after the filing date of the provisional application Russell claims priority to (April 16, 2003), yet is before the filing date of Russell (April 15, 2004). Thus, determining which material in Russell may be entitled to the provisional application filing date depends on the contents of the provisional application. Applicant attempted to view the provisional application using Public PAIR to determine what material in Russell is entitled to the filing date of April 16,

2003; however, it appears to Applicant that either the wrong provisional application was submitted to the USPTO, or the USPTO misfiled the provisional application. For example, when the provisional application no. 60/463,706 is accessed with Public PAIR, a seemingly unrelated provisional application appears (it appears to be a provisional application regarding fiber lasers). The provisional application cover sheet seemingly does not match the specification and drawings (the provisional application number and filing date are stamped on each page, yet the attorney docket number and title on the cover sheet does not match the attorney docket number and title on the specifications and drawings). Applicant invites the Examiner to view the provisional application, and this discrepancy, through Public PAIR. Applicant respectfully requests the assistance of the USPTO in resolving this matter (e.g., determining whether an incorrect specification was transmitted to the USPTO, or locating the correct provisional application). Applicant has no way of determining what material in Russell, if any, may be entitled to the provisional application filing date without USPTO assistance. Furthermore, according to the cover sheet of the provisional application on file, the specification of the provisional application is only 4 pages and has no figures; Russell has 8 columns (without the claims) and 5 figures; suggesting that if the appropriate provisional specification exists, it does not disclose everything in Russell. As such, unless the USPTO can identify that there is a different priority document to review, Applicant respectfully submits that all the content of Russell is not entitled to the filing date of the provisional application but is only entitled to the filing date of Russell; and thus Russell is not prior art. However, for this response, Applicant assumes that the USPTO will resolve this discrepancy and assumes that Russell is entitled to the filing date of the provisional application; however, in future responses (e.g., an appeal), Applicant will not assume that Russell is entitled to the filing date of the provisional application.

Office Action does not address all Required Claim Limitations

Applicant respectfully submits that the Office Action fails to address all required claim limitations on several different occasions in the present Office Action.[1] Applicant will point out these deficiencies claim by claim below. Applicant respectfully requests clarification of the rejections upon these points if the rejections are maintained.

Proposed Combination Renders Morkel Unsatisfactory For Its Intended Purpose

Applicant respectfully submits that it would not have been obvious for one of ordinary skill in the art at the time of the invention to combine Morkel and Livingston and/or Russell as proposed by the Office Action, since the proposed combination renders Morkel unsatisfactory for its intended purpose.[2]

Morkel describes a system that allows an email sender to control the time and frequency of sending updates of personal information (contact information) to select recipients and to securely protect the access of that personal information so that the personal information is received only by the selected recipients (Col 2, lines 4-10). The personal contact information of a user is stored on a server (Col 4, lines 12-18; server 17). The sender typically hashes a recipient's email address and transmits this to the server (see Morkel, Arrow 1 in Figure 1A), and the server associates this hash with the personal contact information (Col 3, lines 2-8). A sender transmits an email to a recipient which includes an indication that contact information is available to that recipient (Col 2 lines 31-35; Arrow 4 in Figure 1A). The recipient receives the email and, after determining it wants the contact information, accesses the server (e.g., by clinking on a URL link in the received email) where the access further includes the recipient transmitting either a hashed version of the recipient's email address, or the raw unhashed recipient's email address (the server then hashes the recipient's email

[1] MPEP § 2143.03, All Claim Limitations Must Be Considered, "All words in a claim must be considered in judging the patentability of that claim against the prior art."
[2] MPEP § 2143.01(V), The Proposed Modification Cannot Render the Prior Art Unsatisfactory For Its Intended Purpose, "If proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification."

address) (Col 6, lines 40-49; Figure 1A, arrow 5). The server compares the stored hash of the recipient's email address (transmitted by the sender) and the hash of the recipient's email address provided by the intended recipient. If the two hashes match, the server has verified that this particular recipient may receive the personal information and forwards the personal information to that recipient (Col 2, lines 43-46; Col 6, lines 45-49; Figure 1A, arrow 6). Thus, Morkel's intended purpose is to facilitate transmission of personal information to select recipients in a secure fashion. Morkel does not describe a do-not-email list or a do-not-contact list, or any other spam prevention mechanism.

Livingston describes a "do not email" list where a "spammer must contact the domain name registrant for every email address on their list" so as to exclude recipients from a mailing list (Paragraph 3). Livingston also states "I feel that a 'do not email' list would work well; unfortunately, such a list could be seriously abused" (Paragraph 4, emphasis added). Thus, Livingston did not perceive there was a solution to the potential of serious abuse of a "do not email" list.

Russell describes a system for telemarketers to screen and block certain messages (e.g., certain phone calls). For example, messages are filtered through a "do not contact list" and if the intended recipient is on that list, the system will block that message. Furthermore, Russell describes sharing unhashed messages between parties (Russell does not describe hashing the messages). Thus, Russell does not offer a solution to the serious abuse of a "do not email" list as recognized by Livingston. Since Livingston and Morkel were publicly available at the time of Russell, and assuming arguendo that Russell was one of ordinary skill in the art, the fact that Russell does not address the serious abuse problem recognized by Livingston is evidence that one of ordinary skill in the art would not have combined the references, for example, because that combination would render Morkel unsatisfactory for its intended purpose (which will be described below).

The Office Action alleges that Morkel describes substantially all of the limitations in the claims except it "fails to disclose use of a do-not-email list, or a master do-not-email list" (Office Action, page 4). Thus, the proposed combination of Morkel and Livingston and/or Russell would have the "do not email" list of Livingston and/or the "do not contact list" of Russell incorporated into Morkel "to design a method further to

include a do not email list in order to provide an efficient anti-spam mechanism" (Office Action, page 4). However, Applicant respectfully submits this proposed combination renders Morkel unsatisfactory for its intended purpose. As stated previously, the intended purpose of Morkel is to facilitate transmission of personal information to select recipients in a secure fashion. The proposed combination modifies Morkel by having the server storing a "do not email" or "do not contact" list which presumably includes hashed versions of email addresses transmitted by the sender (Figure 1A, arrow 1), which the server associates with personal contact information of the sender. In the proposed combination, the sender still transmits an email to an intended recipient indicating that personal information is available, and the intended recipient still accesses the server for that personal contact information. The server then compares those stored hashed values with a hashed value based on an intended recipient's email address.

However, it is unclear to Applicant what the Office Action suggests as occurring as a result of the comparison. One possible interpretation is that when the hashes match, the server will not transmit the personal contact information to the recipient. However, this interpretation renders Morkel's intended purpose of facilitating transmission of personal contact information to select recipients unsatisfactory. For example, the reason the sender transmitted an email message that indicates personal contact information is available to the recipient is for the recipient to access that personal contact information. If the recipient cannot access that personal information (i.e., the server will not send the personal information) Morkel's intended purpose is defeated. Morkel does not even remotely suggest that the server should not transmit the personal contact information to the intended recipient when the intended recipient validates itself (i.e., the sender wants to send the personal contact information to that recipient).

A second possible interpretation is that if the hashes do not match, the server transmits the personal contact information to the recipient. However, this interpretation also renders Morkel's intended purpose of facilitating transmission of personal information to select recipients in a secure fashion unsatisfactory. For example, any hashed version of any recipient's email address that does not match the stored list would be able to receive the personal contact information (i.e,. any email

address not represented on the 'do not contact' list could receive the personal contact information). As previously stated, Morkel's intended purpose is to provide secure access to the personal information only for the selected recipients.

A third possible interpretation is that if the hashes match, the server transmits the personal contact information to the recipient. However, this interpretation would effectively not modify Morkel at all. In addition, it would be illogical for the server to determine to send contact information to the recipient after determining that the recipient's email address is represented on the "do not contact" list.

Furthermore, the sender transmits an email message to the intended recipient with no comparison of any hash values are done, or any spam prevention taken, prior to transmitting that email message (see Figure 1A, arrow 4). Thus, it is illogical for the "efficient anti-spam mechanism" of the proposed combination as suggested by the Office Action to occur after the sender has already transmitted an email message to the recipient.

For at least these reasons, Applicant respectfully submits that the independent claims 29, 67, 71, and 79 are allowable. Applicant respectfully submits that the dependant claims 30-36, 68-70, 72-78, and 80-82 are allowable for at least the reason that they are dependent on an allowable independent claim.

Combination does not teach or suggest required limitations

Applicant respectfully submits that the combination of Morkel, Livingston, and/or Russell, does not teach or suggest the required limitations of Applicant's claims.

As stated previously, the Office Action alleges that Morkel describes substantially all of the limitations in the claims except it "fails to disclose use of a do-not-email list, or a master do-not-email list" (Office Action, page 4). Thus, the proposed combination of Morkel and Livingston and/or Russell would have the "do not email" list of Livingston incorporated into the secure transmission of personal contact information system of Morkel, and/or the "do not contact" database of the telemarketing screen system of Russell incorporated into Morkel.

Claim 29

Applicant respectfully submits that the combination of Morkel, Livingston, and/or Russell does not teach or suggest the required limitations of Claim 29. Claim 29 recites (emphasis added):

> 29. A computer implemented method comprising:
> collecting a set of one or more do-not-email list entries, each do-not-email list entry is a string of characters representing an email address;
> applying a one-way hashing scheme to the set of one or more do-not-email list entries to convert the strings of characters into unique hashed values to create a set of one or more hashed do-not-email list entries, wherein the one-way hashing scheme is intended to conceal the do-not-email list entries from an intended recipient;
> transferring the set of one or more hashed do-not-email list entries to a master do-not-email list server configured to store the set of one or more hashed do-not-email list entries without revealing the email address corresponding to each of the hashed do-not-email list entries;
> requesting from the master do-not-email list server at least one hashed do-not-email list entry from the set of one or more hashed do-not email list entries to create or update a client do-not-email list **on a client machine**;
> causing a client email entry to be hashed using the same one-way hashing scheme to create a hashed client email entry;
> comparing the hashed client email entry to the hashed do-not-email list entries **on the client do-not-email list** to determine whether the hashed client email entry appears on the client do-not-email list; and
> transmitting at least one email to the email address that corresponds to the hashed client email entry upon determining that the hashed client email entry does not appear on the client do-not-email list.

Thus, claim 29 requires a master do-not-email list server storing one or more hashed do-no-email list entries (e.g., a master do-not-email list), a client machine storing a client do-not-email list that is created or updated by requesting from the master do-not-email list server at least one hashed do-not-email list entry (e.g., a separate client do-not-email list on a client machine), a hashing of an email address already in the client's possession (a client email entry) to create a hashed client email entry, and comparing the hashed client email entry to the hashed do-not-email list entries on the client do-not-email list to determine whether the hashed client email entry appears on the client do-not-email list, and transmitting at least one email to the

email address that corresponds to the hashed client email entry upon determining that the hashed client email entry does not appear on the client do-not-email list.

First, the proposed combination does not teach or suggest the limitation "requesting from the master do-not-email list server at least one hashed do-not-email list entry from the set of one or more hashed do-not email list entries to create or update a client do-not-email list **on a client machine**" as required by claim 29 (emphasis added). Firstly, the proposed combination does not teach or suggest requesting a hashed do-not-email list entry from the do-not-email list server. The proposed combination only describes transferring a hashed email address to the server (Morkel, Col 2, lines 37-38). In addition, the proposed combination describes the server storing "a hash of the recipient's e-mail address received from the client" and the "server then forwards the e-mail with the transaction ID to the recipient" (Morkel, Col 2, lines 35-40). Thus, the proposed combination describes the server transferring an email (unhashed) to a recipient, but does not describe the server transferring a hashed email list entry as alleged by the Office Action. Furthermore, the proposed combination does not describe requesting a hashed do-not-email list entry from the master do-not-email list server to create or update a client do-not-email list on a client machine as alleged by the Office Action. Therefore, Applicant respectfully submits that the combination does not teach or suggest "requesting from the master do-not-email list server at least one hashed do-not-email list entry from the set of one or more hashed do-not email list entries to create or update a client do-not-email list **on a client machine**" as alleged by the Office Action, and respectfully requests the rejection be clarified to address this limitation with regard to the combination (e.g., other than simply pointing to Applicant's claim language) if the rejection is maintained.

Second, the proposed combination does not teach or suggest the limitation "comparing the hashed client email entry to the hashed do-not-email list entries **on the client do-not-email list** to determine whether the hashed client email entry appears on the client do-not-email list" as required by claim 29 (emphasis added). It should be noted that a portion of the above limitation was not addressed by the Office Action. For example, the following bracketed portion has not been addressed by the Office Action: "comparing the hashed client email entry to [the hashed do-not-email list entries on the]

client do-not-email list" (Office Action, page 4). The proposed combination fails to teach or suggest the above limitation without the bracketed material, and even more so with the bracketed material. While the proposed combination describes the server comparing a stored hash of a recipient's email address with a computed hash of the recipient's email address, and if the hashes match transmitting contact information to the recipient, the proposed combination does not describe comparing any hashed email entries to other hashed do-not-email list entries on the client do-not-email list. Simply put, the proposed combination describes only the server comparing hashed email entries (Morkel, Col 2 lines 39-46; Col 2 lines 54-58). In contrast, claim 29 requires comparison against the client do-not-email list, which is on the **client machine**.

Third, the Office Action fails to address the limitation "transmitting at least one email to the email address that corresponds to the hashed client email entry upon determining that the hashed client email entry does not appear on the client do-not-email list" as required by claim 29 (emphasis added). Applicant respectfully requests clarification of the rejection to address this limitation if the rejection is maintained.

Thus, certain limitations have not been addressed by the Office Action, certain limitations that were addressed by the Office Action are not taught or suggested by the proposed combination, and these limitations are not obvious in view of the combination for at least the following two reasons.

First, Applicant's claimed invention allows significant advantages as compared to the combination proposed by the Office Action. To illustrate Applicant's claimed invention and by way of example and not limitation, there are two lists each controlled by different parties (e.g., one list controlled by the government and the other list controlled by an email marketer). The content of the two lists is not shared between the parties, but the lists are compared to each other to discover which entries from the second list (e.g., email marketer's list) are also on the first list (e.g., the government's list). The lists are email addresses controlled by the two different parties. The email addresses are confidential, and the comparison is for the purposes of not transmitting email to matching entries. It is accomplished through hashing each entry on both lists; tracking unhashed entries for the second list (e.g., the email marketer's list) and the correspondence between the unhahsed entries and their counterpart hashed values; comparing the hashed entries of

the two lists; and then correlating the results back to the original unhashed second list of email addresses. Each email address determined to be on the first list (e.g., the government's list) will not receive an email (e.g., the email marketer does not send email to the email address determined to be on the government's list).

To say it a different way, by way of example and not limitation, an email marketer has one list of email addresses that the email marketer wants to contact for marketing purposes and another party, in our example the government, has their own list of email addresses that make up a do-not-contact list. The email marketer is not allowed to contact email addresses that choose to opt out of email marketing (i.e., the email addresses on the government's list) so the email marketer desires to check the entries on the government's list to determine if the email marketer should remove an entry from their list. However, the government does not want to share their list of unhashed email addresses that do not wish to be contacted as this information can be very valuable to unscrupulous email marketers (e.g., if the list of unhashed email addresses were compromised, then unscrupulous email marketers could contact the email addresses of people that do not wish to be contacted). Additionally, the email marketer also does not want to share their list of unhashed email addresses because this information is also very valuable to the email marketer and they do not want this list to be public for fear of unscrupulous email marketers (e.g., for the same reasons as above). Therefore, in Applicants' claimed invention a one-way hashing scheme is used by both entities (government and email marketer) such that each entity will have a list containing hashed entries. These two lists can then be compared and matches determined. Thus, with Applicants' claimed invention, for example, the underlying content of the lists (i.e., the email addresses represented by the hashed values on both lists) can be compared (e.g., by comparing the hashed entries on both lists) (in order for the email marketer to determine which email address shall not be contacted) without either party sharing their list of unhashed email addresses. In other words, the government does not trust sharing its unhashed email addresses with the email marketer; and similarly the email marketer does not trust sharing its unhashed email addresses with the government. However, since it is nearly mathematically impossible for an unhashed email address to be determined solely from examining a one way hashed email address, each party (e.g., the government and

the email marketer) is willing to share one way hashed email addresses with each other for comparison purposes.

Secondly, as recognized by Livingston, "a do-not email list would well; unfortunately, such list could be seriously abused" (Livingston, Paragraph 4, emphasis added). Thus, Livingston did not perceive there was a solution to the potential of serious abuse of a "do not email" list. Furthermore, Russell describes sharing unhashed messages between parties (Russell does not describe hashing the messages). Thus, Russell does not offer a solution to the serious abuse of a "do not email" list as recognized by Livingston. Since Livingston and Morkel were publicly available at the time of Russell, and assuming arguendo that Russell was one of ordinary skill in the art, the fact that Russell does not address the problem of serious abuse is evidence that either the combination is not proper (see prior argument) and/or the combination of the references do not satisfy the abuse problem and the limitations of Applicant's claims are not found in the combination (e.g., the limitations of Applicant's claims solve the serious abuse problem).

Thus, Applicant respectfully submits that the combination of Morkel, Livingston, and/or Russell, does not teach or suggest the required limitations of claim 29. Thus, Applicant respectfully requests withdrawal of the rejection and allowance of the claim.

In addition, Applicant respectfully submits that the dependant claims 30-36 depend on claim 29 and are allowable for at least the same reason.

Claims 67 and 71

As discussed previously, the Office Action alleges that Morkel describes substantially all of the limitations in the claims except it "fails to disclose use of a do-not-email list, or a master do-not-email list" (Office Action, page 4). Thus, the proposed combination of Morkel and Livingston and/or Russell would have the "do not email" list of Livingston incorporated into the secure transmission of personal contact information system of Morkel, and/or the "do not contact" database of the telemarketing screen system of Russell incorporated into Morkel.

Applicant respectfully submits that the combination of Morkel, Livingston, and/or Russell does not teach or suggest the required limitations of Claim 67 or Claim 71. Claim 67 recites (emphasis added):

> 67. A computer implemented method to identify email addresses registered on a do not contact list that are in a client's list without revealing the email addresses on the do not contact list or the client's list comprising:
>
> the client encrypting at least certain of entries on the client's list to create a plurality of encrypted entries, where each entry includes at least an email address, wherein the entries are encrypted in a way that it is intended that an intended recipient cannot decrypt the entries;
>
> the client transmitting over a network said plurality of encrypted entries from the client's list to a service for comparison to encrypted entries of the do not contact list, wherein the encrypted entries of the do not contact list were formed by encrypting information, including at least an email address, a matching of an encrypted entry from said plurality of encrypted entries from the client's list to an entry of the do-not-contact list represents that the underlying email address needs to be identified;
>
> the client receiving results of the comparison, wherein the results of the comparison are an indication of which encrypted entries on the client's list match the encrypted entries on the do not contact list, and the results are not unencrypted entries of the do not contact list; and
>
> the client transmitting at least an email to the email addresses in the client's list that correspond to the encrypted entries on the client's list that did not match the encrypted entries on the do not contact list.

Thus, claim 67 requires two lists: a do not contact list and a client's list, each including a plurality of email addresses. Each list is encrypted (e.g., hashed). The client transmits its encrypted entries to a service for comparison to encrypted entries of the do not contact list. The client receives result of the comparison which indicate which of its encrypted entries match the encrypted entries on the do not contact list, and the client transmits an email to an email address whose encrypted entry did not match any of the encrypted entries on the do not contact list.

First, the proposed combination does not teach or suggest the limitation "the client receiving results of the comparison, wherein the results of the comparison are an indication of which encrypted entries on the client's list match the encrypted entries on the do not contact list, and the results are not unencrypted entries of the do not contact list" as required by claim 67 (emphasis added). It should be noted that the following

portion of this limitation: "wherein the results of the comparison are an indication of which encrypted entries on the client's list match the encrypted entries on the do not contact list, and the results are not unencrypted entries of the do not contact list" was not addressed in the Office Action.[3] If this rejection is maintained, Applicant respectfully requests that this part of the limitation be addressed. Applicant respectfully submits that the proposed combination does not teach or suggest the above limitation without the missing portion of the limitation and even more so with the missing portion of the limitation. The proposed combination describes if the hashes match, the server transmitting personal contact information to the recipient (Morkel, Col 2, lines 47-58). However, the proposed combination does not teach or suggest the client receiving results of the comparison. In other words, in the proposed combination, the server is not comparing the hashes for the client, but rather is comparing a recipient's email address hash to determine if the recipient may receive the personal contact information (i.e., the comparison is performed to verify the recipient's identity). Thus, in the proposed combination, the client does not receive results of the comparison. Therefore, Applicant respectfully submits the proposed combination does not teach or suggest "the client receiving results of the comparison, wherein the results of the comparison are an indication of which encrypted entries on the client's list match the encrypted entries on the do not contact list, and the results are not unencrypted entries of the do not contact list" as required by claim 67 (emphasis added).

Secondly, the proposed combination does not teach or suggest the limitation "the client transmitting at least an email to the email addresses in the client's list that correspond to the encrypted entries on the client's list that did not match the encrypted entries on the do not contact list" as required by claim 67 (emphasis added). It should be noted that this limitation was not addressed by the Office Action. If this rejection is maintained, Applicant respectfully requests that this part of the limitation be addressed. Nevertheless, Applicant respectfully submits that the proposed combination does not teach or suggest the above limitation. To illustrate, in Applicant's claimed invention, after receiving the results of the comparison, the client transmits at least an email to an email address in the client's list whose corresponding encrypted entry did not match any

[3] See Office Action, page 7.

of the encrypted entries on the do not contact list. Thus, the email addresses whose corresponding encrypted entries in the client's list did not match the encrypted entries on the do not contact list are safe for the client to email (e.g., those email addresses have not opted out of receiving email).

Thus, certain limitations have not been addressed by the Office Action, certain limitations that were addressed by the Office Action are not taught or suggested by the proposed combination, and these limitations are not obvious in view of the combination for at least the reasons as discussed with reference to claim 29.

Thus, for at least the above reasons, Applicant respectfully submits that the combination of Morkel, Livingston, and/or Russell, does not teach or suggest the required limitations of claim 67. Thus, Applicant respectfully requests withdrawal of the rejection and allowance of the claim.

In addition, Applicant respectfully submits that the dependant claims 68-70 depend on claim 67 and are allowable for at least the same reason.

Regarding claim 71, Applicant respectfully submits that claim 71 includes similar limitations as claim 67 with the addition that "the encrypted entries of the do - not-contact list were formed by encrypting information, including at least an email address that belongs to a minor" (claim 71, emphasis added).

Thus, Applicant respectfully submits that the combination of Morkel and Livingston does not teach or suggest the required limitations in claim 71 for at least the same reasons as claim 67.

Applicant respectfully submits that the dependant claims 72-78 depend on claim 71 and are allowable for at least the same reason.

Claim 79

Applicant respectfully submits that the combination of Morkel, Livingston, and/or Russell does not teach or suggest the required limitations of Claim 79. Claim 79 recites (emphasis added):

Claim 79. A computer implemented method to identify email addresses registered on a do-not-contact list without revealing the email addresses on the do-not-contact list comprising:

a client encrypting at least certain of entries on the client's list to create a plurality of encrypted entries, where each encrypted entry includes at least an email address that does not wish to be contacted, wherein the entries are encrypted in a way that it is intended that an intended recipient cannot decrypt the entries;

the client causing a comparison of said plurality of encrypted entries from the client's list to a plurality of encrypted entries of a master do-not-contact list, wherein the encrypted entries of the master do-not-contact list were formed by encrypting information, including at least an email address that belongs to a minor, a matching of an encrypted entry from said plurality of encrypted entries from the client's list to an entry of the master do-not-contact list represents that the underlying email address needs to be identified;

the client receiving results of the comparison, wherein the results indicate at least one of the entries on the client's list is not on the master do-not-contact list, and the results do not reveal the email addresses on the master do-not-contact list;

the client updating the client's list with the results to remove the at least one of the entries on the client's list that is not on the master do-not-contact list; and the client transmitting at least an email to the at least one email address that corresponds to the removed entry.

First, claim 79 was summarily rejected by the Office Action as reciting the limitation of claims 29 and 67 and therefore rejected for the same reasons as claims 29 and 67 (Office Action, page 7). However, Applicant respectfully submits that claim 79 includes distinct and different limitations than those in claims 29 or 67. For example, unlike claim 29 or claim 67, claim 79 requires "a client encrypting at least certain entries on the client's list to create a plurality of encrypted entries, where each encrypted entry includes at least an email address that does not wish to be contacted" (emphasis added). Thus, in claim 79, the client's list includes unencrypted email addresses that do not wish to be contacted (e.g., email addresses previously determined to be on a master do not contact list) and these entries are then encrypted. These encrypted entries of the client are compared with encrypted entries of the master do not contact list for the purpose of verifying whether the entries of the client are still on the master do not contact list (i.e., whether the unencrypted email addresses still do not wish to be contacted). As another example, unlike claim 29 or claim 67, claim 79

requires "the client updating the client's list with the results to remove the at least one of the entries on the client's list that is not on the master do-not-contact list" (emphasis added). Applicant respectfully requests clarification of the rejection if the rejection is to be maintained.

Second, Applicant respectfully submits that the combination of Morkel, Livingston, and/or Russell does not teach or suggest the limitation "the client receiving results of the comparison, wherein the results indicate at least one of the entries on the client's list is not on the master do-not-contact list, and the results do not reveal the email addresses on the master do-not-contact list" as required by claim 79 (emphasis added). The proposed combination describes if the hashes match, the server transmitting personal contact information to the recipient (Morkel, Col 2, lines 47-58). However, the proposed combination does not teach or suggest the client receiving results of the comparison. In other words, in the proposed combination, the server is not comparing the hashes for the client, but rather is comparing a recipient's email address hash to determine if the recipient may receive the personal contact information (i.e., the comparison is performed to verify the recipient's identity).

Third, Applicant respectfully submits that the combination of Morkel, Livingston, and/or Russell does not teach or suggest the limitation "the client updating the client's list with the results to remove the at least one of the entries on the client's list that is not on the master do-not-contact list; and the client transmitting at least an email to the at least one email address that corresponds to the removed entry" as required by claim 79 (emphasis added). The proposed combination does not teach or suggest that the client remove an entry from its list that is not on the master do not contact list. The proposed combination only describes, as a result of the comparison, transmitting personal information to the recipient if the hashes match, and presumably not transmitting the personal information to the recipient if the hashes do not match.

Thus, certain limitations have not been addressed by the Office Action, certain limitations that were addressed by the Office Action are not taught or suggested by the proposed combination, and these limitations are not obvious in view of the combination for at least the reasons as discussed with reference to claim 29.

Thus, for at least the above reasons, Applicant respectfully submits that the combination of Morkel, Livingston, and/or Russell, does not teach or suggest the required limitations of claim 79. Thus, Applicant respectfully requests withdrawal of the rejection and allowance of the claim.

In addition, Applicant respectfully submits that the dependant claims 80-82 depend on claim 79 and are allowable for at least the same reason.

CONCLUSION

Applicant respectfully submits that all rejections have been overcome and that all pending claims are in condition for allowance. If there are any additional charges, please charge them to our Deposit Account Number 02-2666. If a telephone conference would facilitate the prosecution of this application, Examiner is invited to contact Daniel M. DeVos at (408) 720-8300.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: April 1, 2008

/Daniel M. De Vos/
Daniel M. DeVos
Reg. No. 37,813

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(408) 720-8300